Aker Secure Roaming User's Manual

- Introduction
- 1 - Installation
  - 1-1 System requirements
  - 1-2 Installation
  - 1-3 Removal
- 2 - Secure Roaming Server
  - 2-1 Server configuration page
  - 2-2 Client configuration page
  - 2-3 Filtering configuration page
  - 2-4 Active clients page
  - 2-5 Certificate Authority page
  - 2-6 Log page
  - 2-7 About page
- 3 - Secure Roaming Client
  - 3-1 Servers page
  - 3-2 Certificates
  - 3-3 Requests page
  - 3-4 Tokens page
  - 3-5 Log page

Copyright (c) 2003-2005 Aker Security Solutions

Introduction

This is the Aker Secure Roaming user's manual. In the following chapters you will learn how to install and configure the product. This introduction describes the manual's organization and the conventions used writing it.

What is the Aker Secure Roaming?

The Secure Roaming system makes it possible for remote users to connect to a server and establish a secure channel (VPN) to the home network. This VPN is special in that it assigns a home-network IP address to the client, enabling the user to work exactly the same way he does when his not roaming.

Two products make up the system:

- **Aker Secure Roaming Server**

  The server runs over Windows 2000 or better, Linux with kernel 2.4 series and FreeBSD 4.9 or better.
  It accepts the connections and sets the user's network configuration according to pre-defined parameters, making the connection setup experience very simple for the end-user.

- **Aker Secure Roaming Client**

  The client runs over Windows 98, Windows 2000 or better, Linux with kernel 2.4 series and FreeBSD 4.9 or better.
  It has a very simple user-interface, where not much more apart from the server's IP address should be configured. It can also be setup to synchronize the VPN establishement and teardown with the Windows dialup adapter status.

How is this manual organized?

This manual is made of several chapters. Each one of them explains how to configure some features of the programs. It also explains how to best fine-tune the options presented by it.

Although you may find screeshots from different OSes as yours, the graphical user interfaces (GUIs) look and behave exactly yhe same way in the different OSes, the only remarkable change being the window manager style (*skin*).

We strongly recommend that this manual be read at least once as a whole.

In various places over the manual, you'll find the symbol followed by some red text. This text presents a very important remark which should be completely understood before continuing.

Copyright (c) 2003-2005 Aker Security Solutions

1-0 Aker Secure Roaming Installation

In this chapter you'll learn how to install or remove the Aker Secure Roaming products.

1-1 System Requirements

- **Aker Secure Roaming Server**
    1. Windows 2000 or better
    2. Linux (kernel 2.4.x)
    3. FreeBSD 4.7 or better

- **Aker Secure Roaming Client**
    1. Windows 2000 or better
    2. Windows 98
    3. Linux (kernel 2.4.x) with KDE or Gnome
    4. FreeBSD 4.7 or better with KDE or Gnome

The minimum hardware requirements vary greatly according to the number of simultaneous clients and its link speed. The absolute minimums are the same needed by the above OSes.

The **Client** consumes no more than 5MB of physical memory and is able to perform in speeds at least 100Kb/s without imposing a significant CPU usage on a 500MHz Pentium-2 class CPU.

The **Server** consumes aproximately 50 kB of memory per connected client on top of a base 3MB. It will consume CPU accordingly to the aggregate instantaneous connection speed. As a rule of thumb, you should allow 30MHz of CPU frequency for each Mbit/s aggregate neto (uncompressed) connection speed.

Please note that all computer peripherals must be explicitly supported by the OS.

1-2 Installing the products

The installation should be quite straightforward. Please follow the steps bellow.

Windows installations

Once you have the **`AkerSecureRoaming-client-win-1.5-en.exe`** file, please do:

1. Click on the **Start** button to raise the Start Menu
2. Choose the **Run program...** item

3. Browse to the **`AkerSecureRoaming-client-win-1.5-en.exe`** file and click ok.
4. Follow the simple on screen instructions

Linux installations

On Linux, the Secure Roaming products come as RPM packages. These can be installed by issuing the following command on a shell window:

```
rpm -ivh <package-file-name>
```

Alternaltivelly, you can use a graphical package manager of your choice.

FreeBSD installations

On FreeBSD, the Secure Roaming products come as standard packages. These can be installed by issuing the following command on a shell window:

```
pkg_add <package-file-name>
```

Alternaltivelly, you can use a graphical package manager of your choice.

Note for Linux and FreeBSD users: The graphical user interface uses the QT 3 library. It should be installed automatically when KDE is installed. If it is not, or your version is incompatible, please browse to the download section of the Aker website and fetch the required library.

1-3 Removing the products

Windows installations

1. Open the Control Panel
2. Click on `Add Remove Programs`
3. Chose the Aker Secure Roaming product you wish to remove
4. Click on the `Remove` button
5. Follow the on-screen instructions

Linux installations

To remove the Secure Roaming products from you host, you can either use a graphical package manager, or issue the following command on a shell prompt:

```
rpm -e <package_name>
```

If the package name is unknown, use the following command to find it out:

```
rpm -qa | grep Aker
```

FreeBSD installations

To remove the Secure Roaming products from you host, you can either use a graphical package manager, or issue the following command on a shell prompt:

```
pkg_delete <package_name>
```

If the package name is unknown, use the following command to find it out:

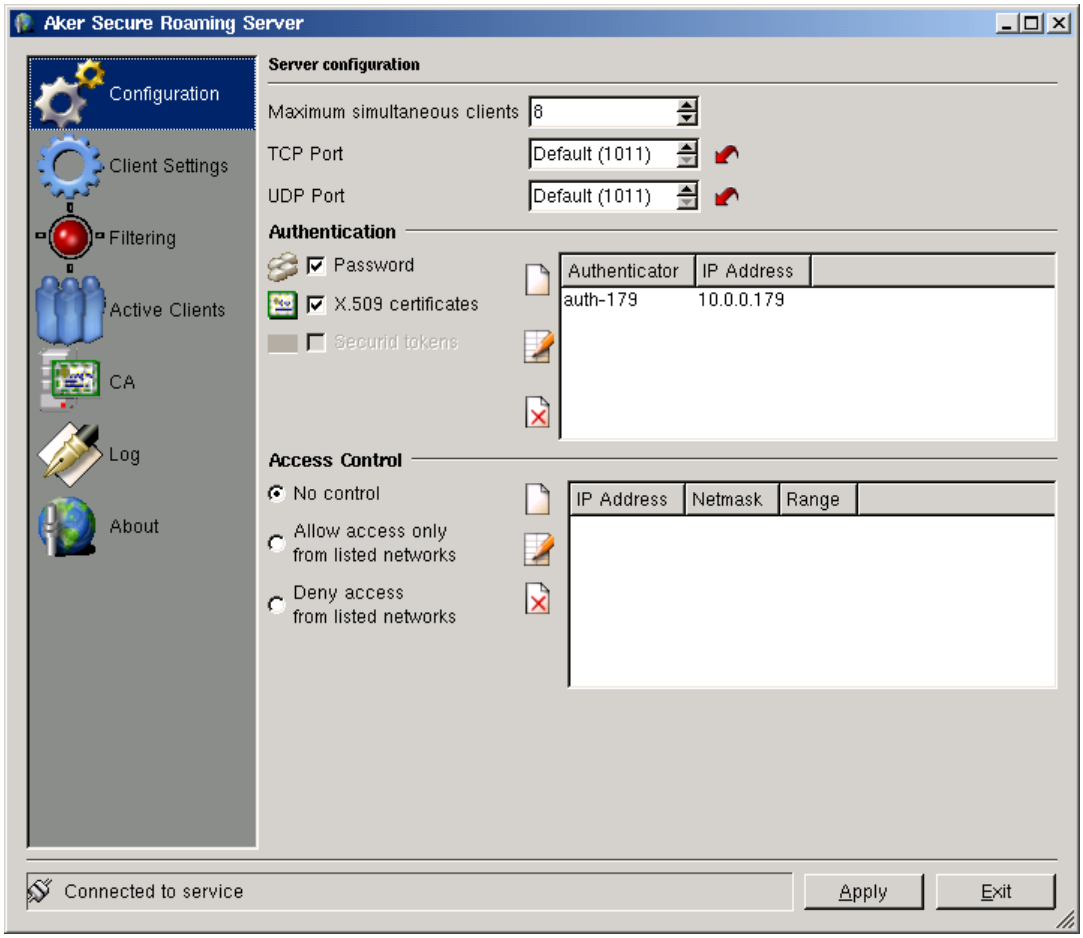
```
pkg_info | grep Aker
```

Copyright (c) 2003-2005 Aker Security Solutions

2-0 Configuring and managing the Aker Secure Roaming Server

Here you'll find the necessary instructions to correctly configure and manage your Secure Roaming Server.

2-1 Server configuration page

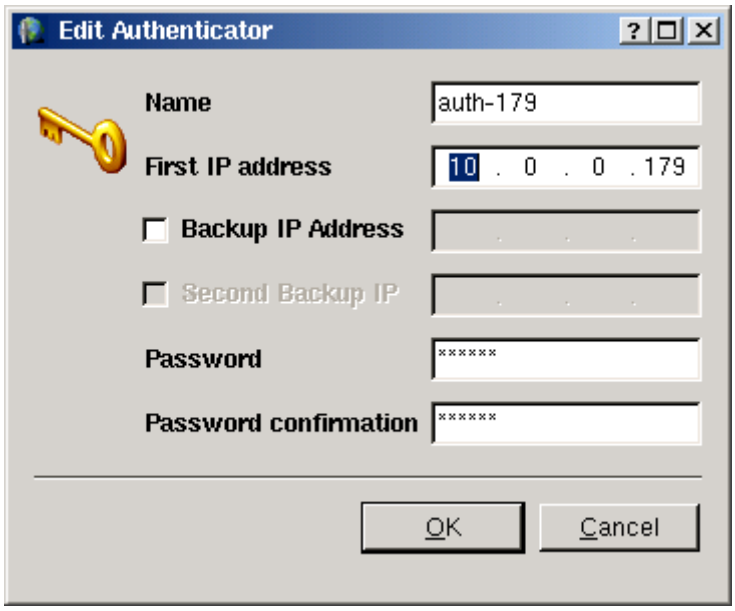


In this page you'll find the settings which are relevant to the server itself:

- **Maximum simultaneous clients**: Here you can set the maximum number of clients allowed to simultaneously connected at any given time. Use this setting to avoid having your server overflooded by too many clients, which could decrease the expected performance.
  Please note this number is limited by your license.
- **TCP / UDP port**: This controls allow you to set which ports the server will use to listen for client connections and data, respectively. For instance, you could set the server to use ports TCP/443 and UDP/53, in order to easily bypass firewalls and/or other filtering devices between your server and clients, which would mistake the VPN connection by a encrypted HTTP request and a DNS request,

respectively.
The default port is **1011** for both TCP and UDP ports.

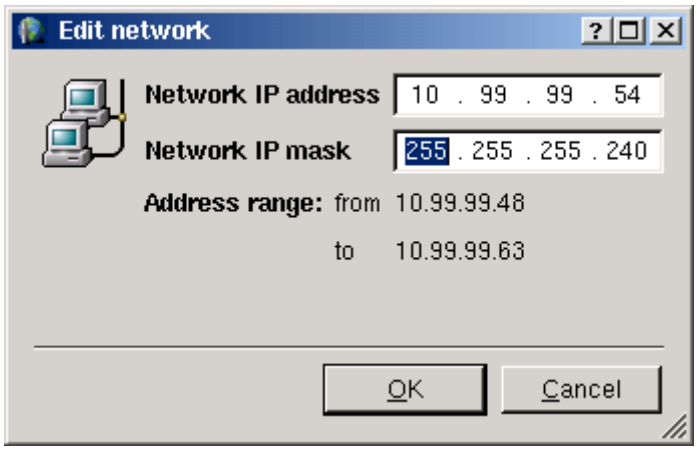
- **Authentication**: Here you can select which authentication methods (the current version supports username/password authenticators and X.509 Certificates) you will allow your clients to use.
  In the right list, you can add, edit or remove the authenticators you will use. An authenticator is a computer which runs the Aker Authentication Agent in order to export its directory in a fully encrypted way. When adding or editing a new authenticator, the following window will appear:



  In this dialog, you can set the name, the primary IP address, the backup ones, and the password for your authenticator. Please remember the password should be the same one you set in the Aker Authentication Agent.
  For more information regarding the Authentication Agent, please refer to the Aker Firewall User's Manual, which can be found on the Aker WebSite.
  In order for the X.509 authentication to work, at leaset one CA (Certificate Authority) must be installed (explained bellow). The clients who present a certificate signed by a trusted CA and prove a corresponding private key ownership will be allowed access. These steps are performed automatically by the Secure Roaming Client.

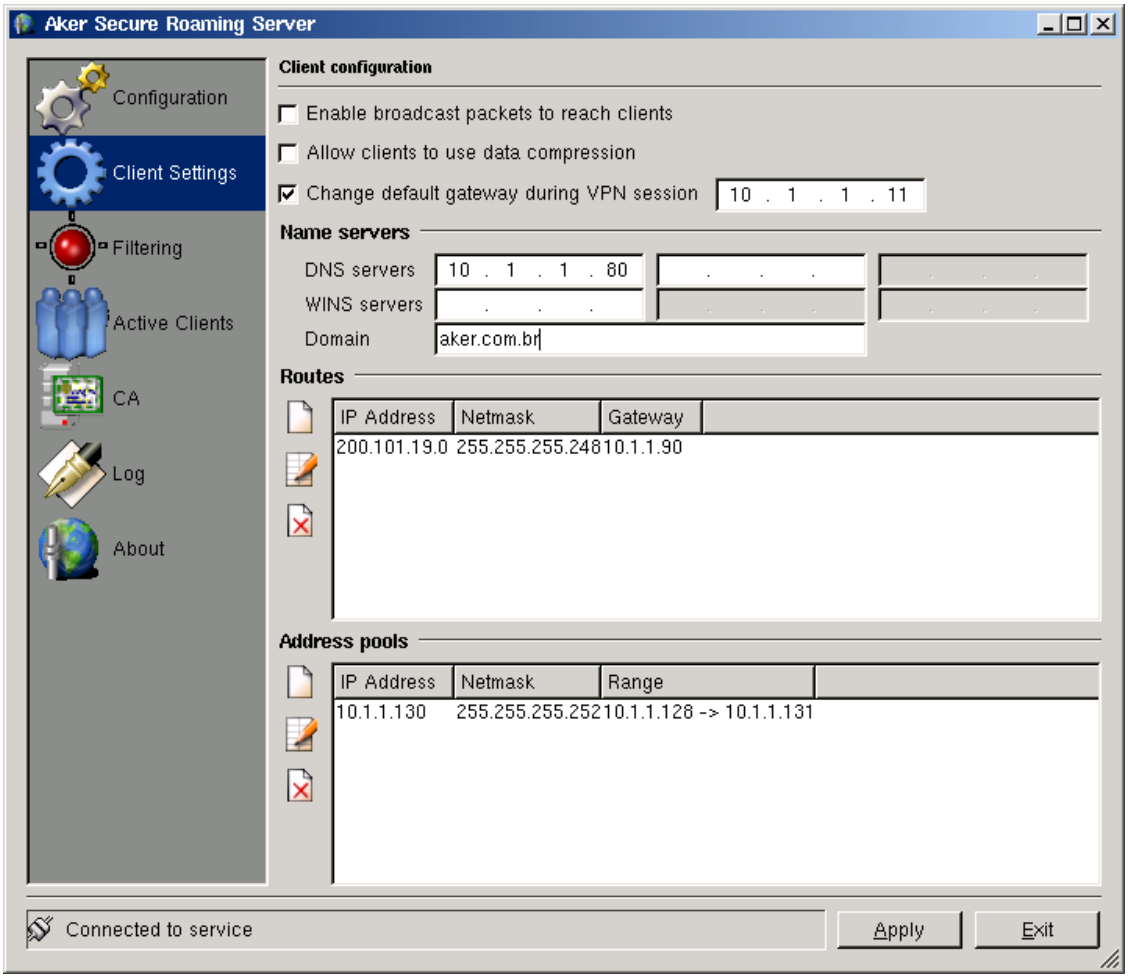
- **Access Control**: Here you can configure from which clients you will accept connections:
  1. **No control**: Every client is allowed to connect to the server.
  2. **Allow access only from listed networks**: Only the clients which have IP addresses belonging to the networks in the right list will successfully establish a VPN.
  3. **Deny access from listed networks**: The clients which have IP Addresses belonging to the networks in the right list will not be able to establish a VPN. Everyone else will.

  By editing or creating a new entry in the right network list, you'll be taken to the following dialog:



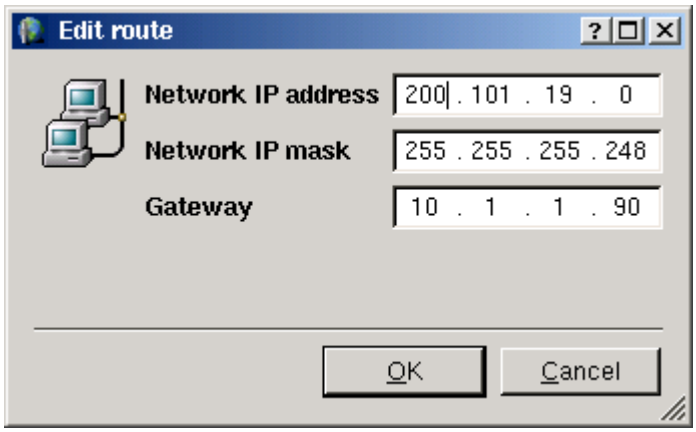
In this window, you will enter the network IP address and netmask. Please note that invalid adresses or netmasks won't be accepted, i.e. you won't be able to type them in.
Once you enter valid address and netmask, the IP address range will be calculated automaticaly. This range **includes** the first (network address) and last (broadcast address) IPs, since it does not specify a subnet in the routing meaning, but a range of IP addresses.

2-2 Client configuration page



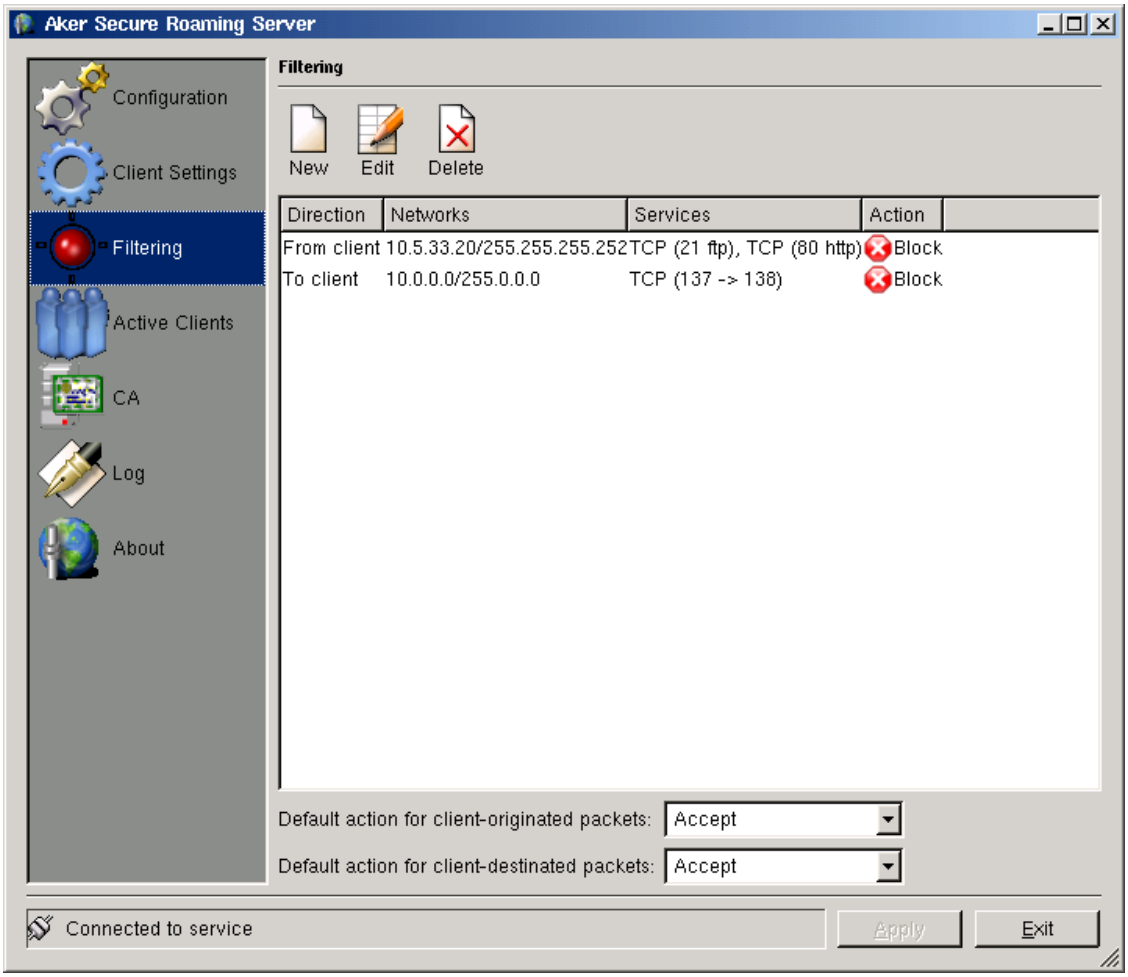
In this page you'll find the settings which are relevant to the clients who connect to the server:

- **Enable broadcast packets to reach clients**: This options disables the block the server imposes on broadcast packets. Broadcast packets may be needed by some protocols like SMB/Netbios (Microsoft Windows networking). On the other hand, a badly configured network will have lots of those packets, which, when allowed to reach the client, could simply flood a typical dial-up link used by roaming users.
- **Allow clients to use data compression.** This option allows for the clients to enable bidirectional data compression, so that the net bandwidth can be increased, specially in very slow connections such as dialup modems.
- **Change default gateway during VPN session**: This option makes the server alter the clients' default gateway setting for the duration of the VPN session. Enabling it will make the client's computer behave exactly how it would when connected inside the network, but will also redirect every traffic from it to the outside to the default router on your network.
If you have a few known routes, it is best to set those in the list bellow, thus letting the Internet-destined traffic to flow directly from the client to it, without consuming your link's bandwidth twice.
- **Name servers**: For the roaming user's computer to behave exactly the same way it does when connected to his home network, it needs to resolve network names using the DNS and WINS services. Please fill them from left to right, noting that the next one will only be available when the previous is filled with a valid IP address (you won't be allowed to type something else than .
As with the default gateway, the client's DNS servers will be restored when the VPN session is terminated.
- **Routes:** When a large intranet is used, clients may need routes to other network segments in order to reach them. When entering a new route or editing an old one, you will be prompted with the following dialog box.



In this window you will be able to enter the network address and mask and the gateway to reach it. Please note it will not be possible to enter invalid IP adresses or masks in the appropriate fields.
- **Address Pools**: The IP addresses assigned to the client will be drawn from the address pools bellow in a sequential fashion. Please note these pools do not specify a network, they specify a range of IP addresses. The dialog to edit them is the same one used to edit the access control lists.

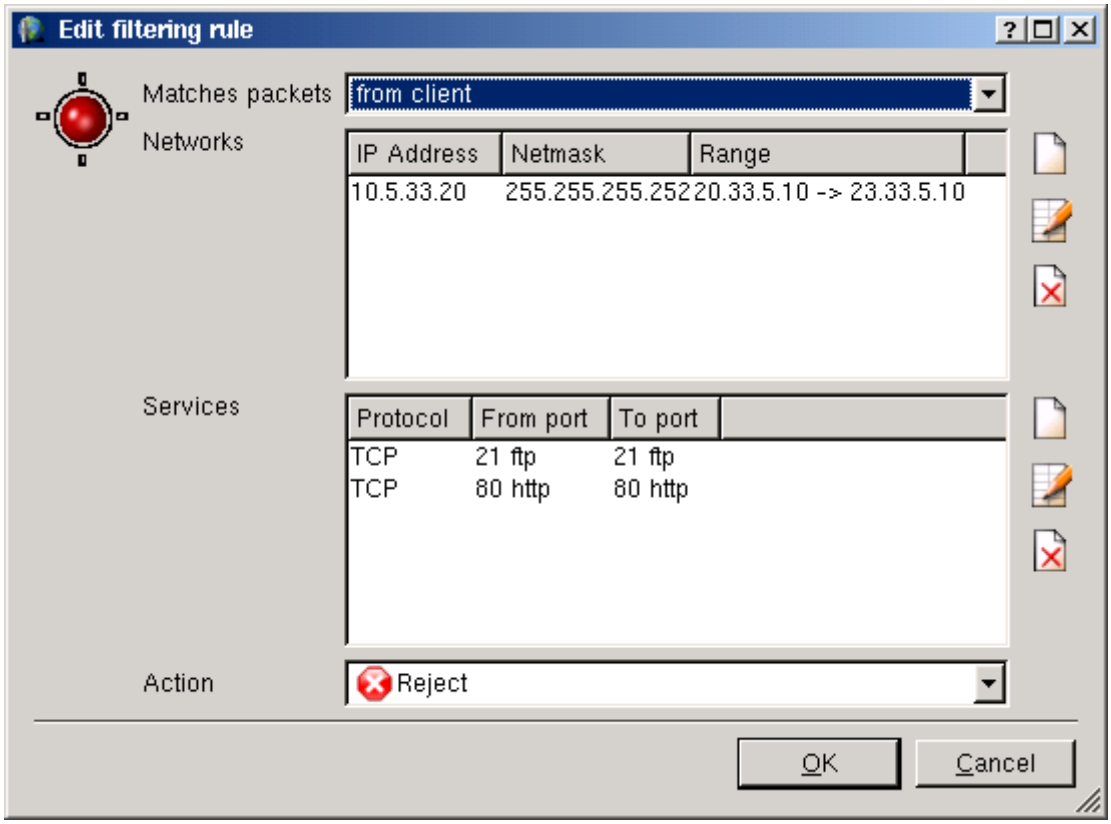
2-3 Filtering configuration page



In this page, you will be able to create filters for the traffic between the client and the home network. This can be used both to enforce security measures and to restrict the traffic of useless data, so that mission-critical information has more of the rather scarce roaming user's connection bandwidth.

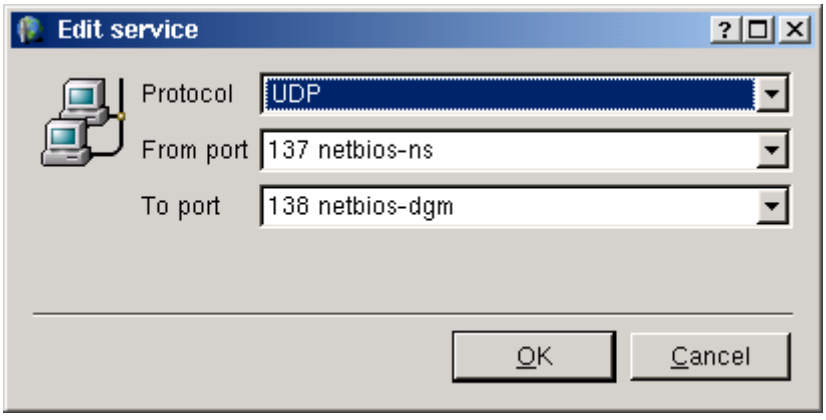
- **Rules list**: In this list you can see the rules currently enforced. There are two kinds of rules:
    1. **Rules for client-originated traffic**, which are marked as *From Client*
    2. **Rules for client-destinated traffic**, which are marked as *To Client*

    The rules can also **block** or **allow** the traffic.
    The rules are scanned sequentially. This means that a more generic rule may eclipse the context of a following more specific one.
    When editing new or old rules, the following dialog will be shown:



In this dialog, the following controls are available:

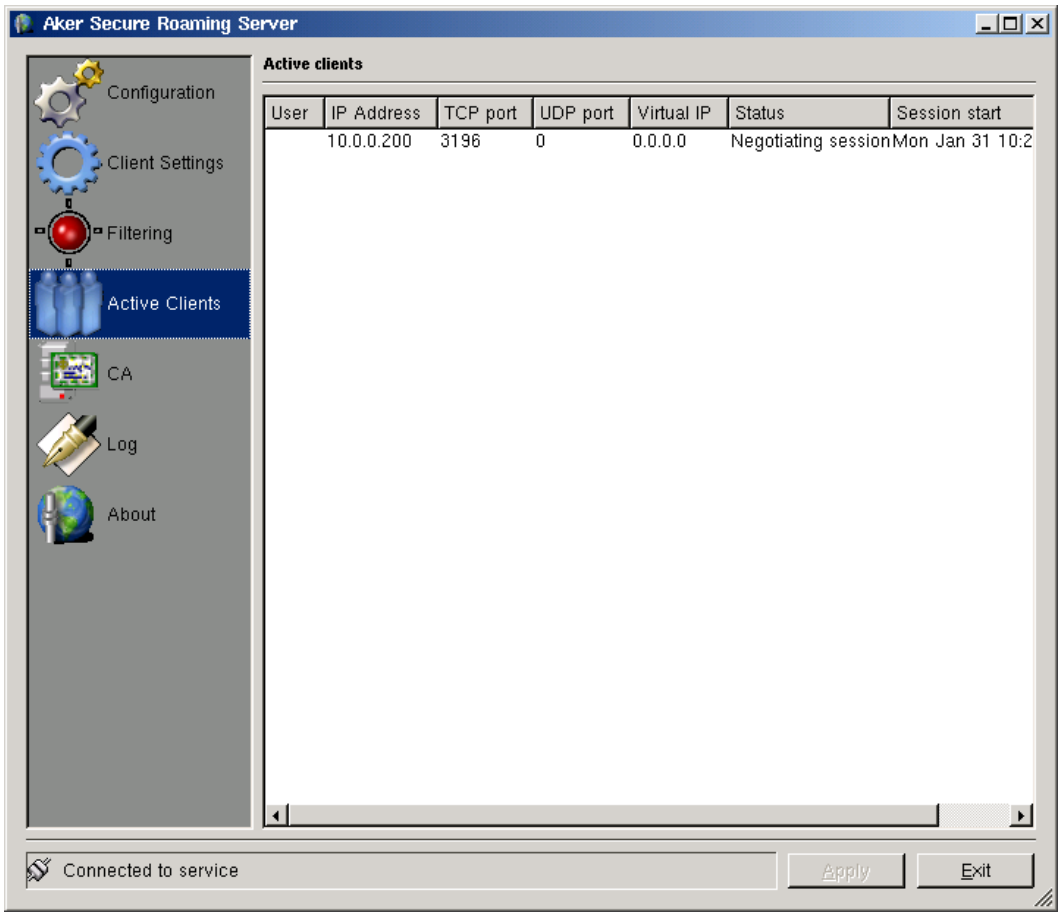
- **Matches packets**: Here you can set the type of rule to either client-originated packets (**from client**)or client-destinated packets (**to client**).
- **Networks**: This list contains the networks where the other IP address (destination IP address for client-originated rules or source IP address for client-destinated rules) should be for it to match. These can be edited using the same dialog used to edit the access control lists.
- **Services**: This list contains the services (*destination port* on TCP or UDP packets, *type of service* on ICMP packets or *protocol* on raw IP packets) which should be present on the packet for the rule to match.
  You can edit these using this dialog:



        - **Protocol**: this is the type of IP packet you wish the service to specify, i.e. the definition of service you are wishing to use from the above ones.
        - **From port / To port**: The services for which the rule will match are the ones with numbers (port, type of service, or protocol) between these two, inclusive.
    - **Action**: Defines if the rule will allow or deny the packet to transverse the VPN.

      The rules are checked both at the client and at the server. This ensures both maximum performance (no packet enters the VPN to be discarded at the other end) and maximum security (event a malicious client won't be able to inject disallowed traffic into the network).
- **Default actions**: These can be understood as a default last rule action, which applies to every packet which for the rules didn't match.

2-4 Active clients page

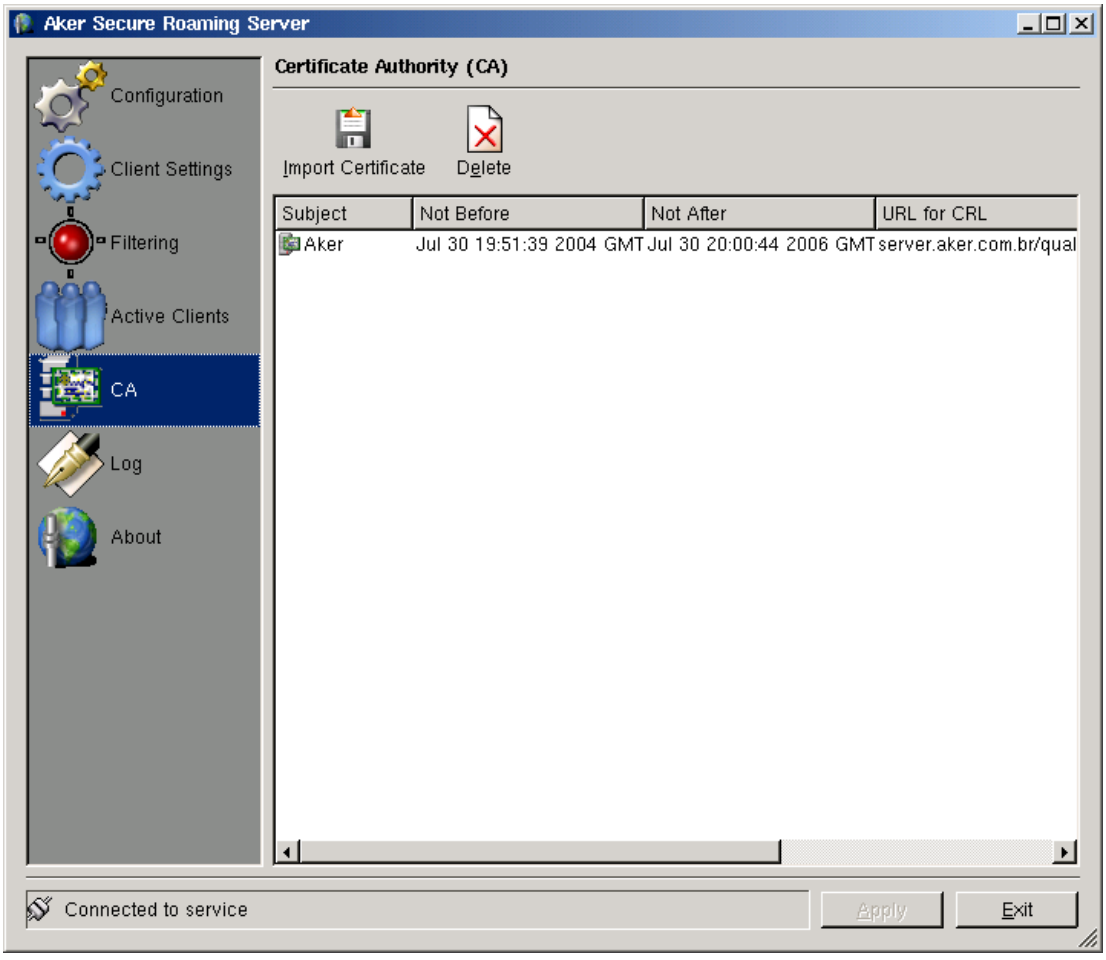


Here you can see the clients which are connected right now and their properties:

- **Username**: This field includes the username and authenticator the user used to log in. It can also contain some other information pertinent to the other authentication methods.

- **IP address**: This field shows the address from which the client has connected, as seen from the server. Beware the client can be behind a IP-masquerading device, which could effectively hide the real address he is using.
- **TCP / UDP port**: This field displays the ports from which the client is connecting. The above note applies here too, i.e., the numbers could be altered by a IP-masquerading device
- **Virtual IP**: This field shows the IP address which has been assigned to the client from the previously defined pool.
- **Status**: In this field you will find a text describing the VPN status. The important ones are *Authenticating*, which means the client provided authentication data and we are waiting for a positive response from the authenticator, and *Established*, which means the client is fully functional.
- **Session start**: This field shows the date and when time the client connected.

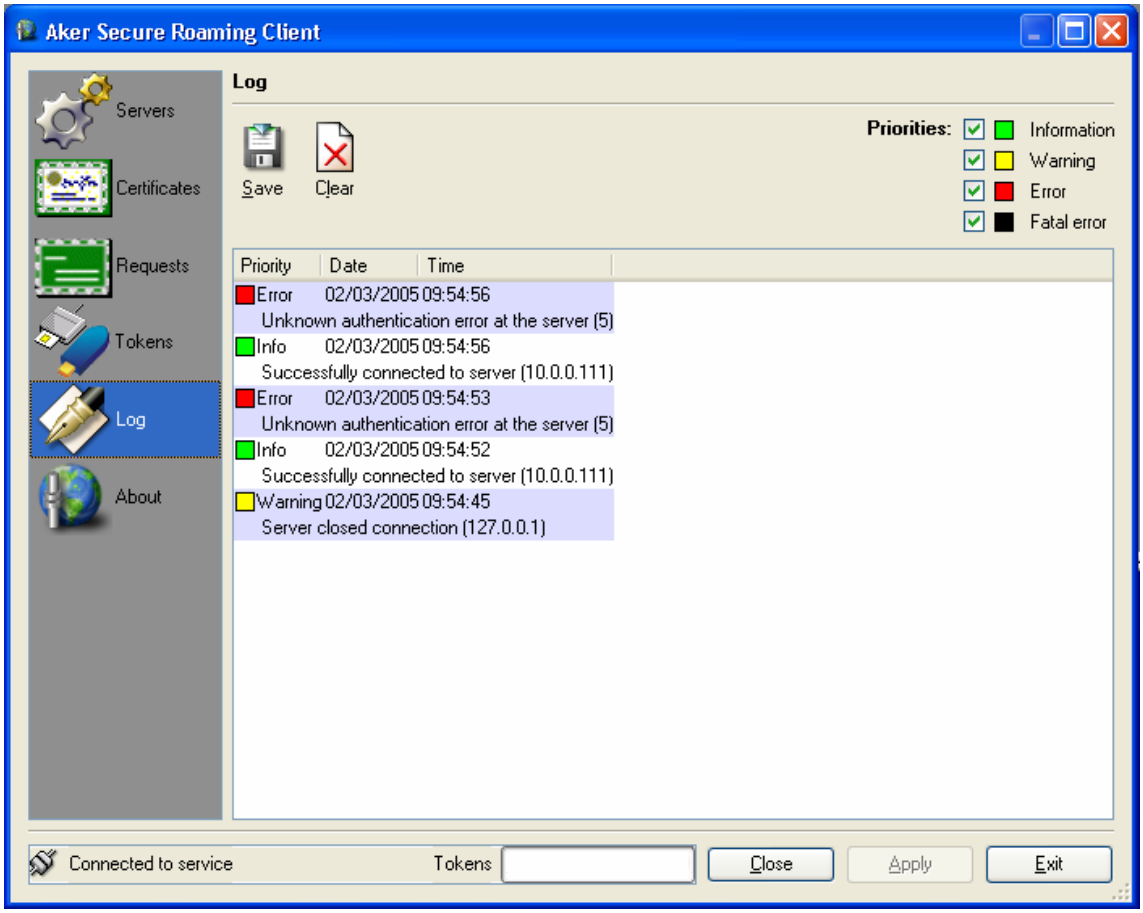
2-5 Certificate Authority Page



Here you can define which CAs you trust. This trust relation implies that every valid certificate issued by the CAs will be accepted as valid credentials for VPN establishment purposes.
To add a CA to the trusted CAs list, click on the Import Certificates button, find its X.509 certificate and click OK.
You can also assign a location (URL) where Secure Roaming Server will periodically download the CA's CRL (Certificate Revocation List) from. Whenever a certificate is

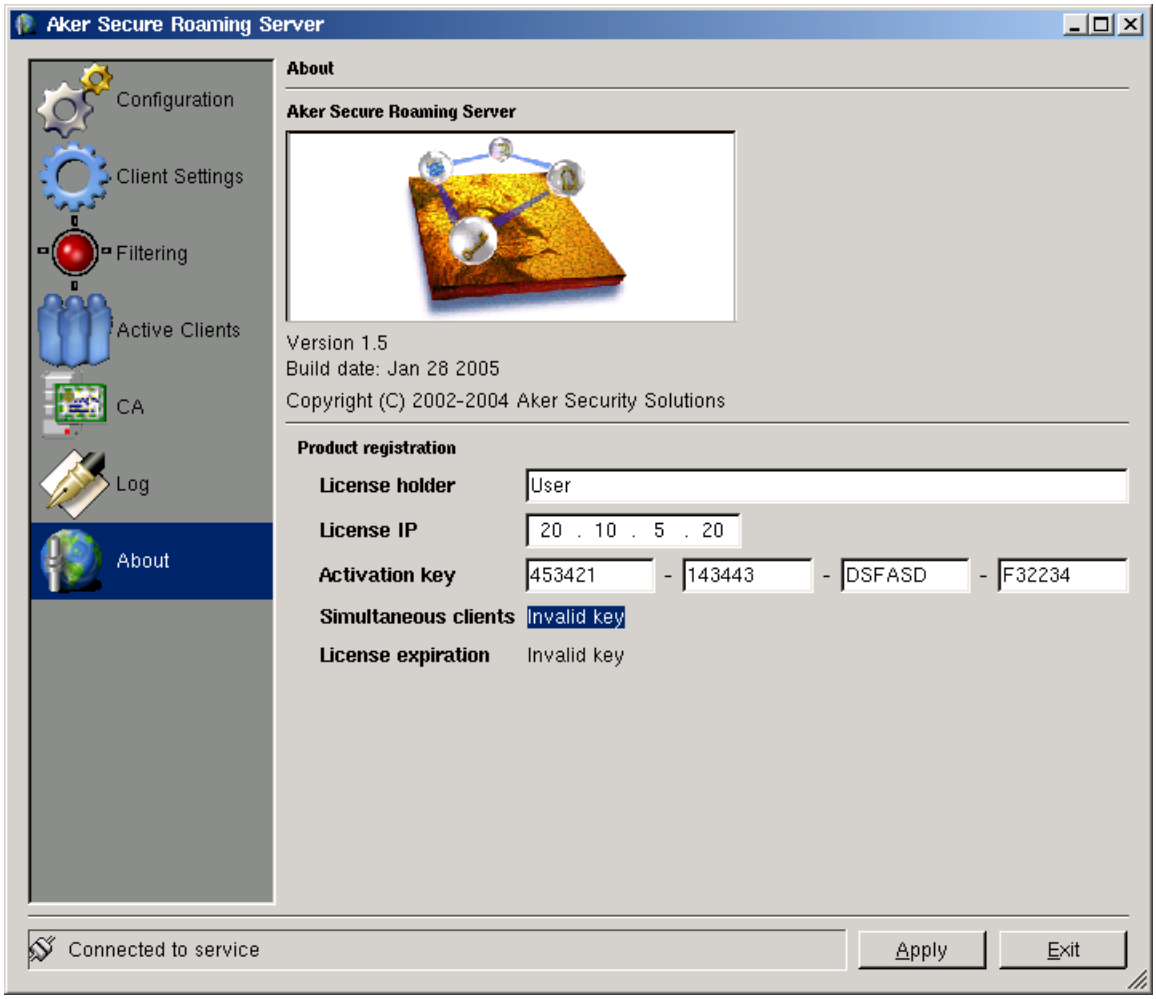
no longer to be accepted (e.g. when its corresponding private key has been compromised), the CA will publish its serial number on its CRL. Secure Roaming Server will not accept certificates which are listed as canceled, no mater the reason. To define the URL where the CRL is to be found, right-click on the corresponding CA line and enter on the pop-up menu. The CRL will be downloaded upon service startup and each 24 hours.

2-6 Log page



Here you can examine the system log and set wherever it will be sent to syslog (Unix) or Event Viewer (Windows).
The syslog facility combo box (only in Unix Systems) defines which syslog facility the Aker Secure Roaming Server should use.

2-7 About page



In this last page, you must set the registration information according to the license you received from Aker Security Solution. Please verify the limits (maximum number of simultaneous clients and date of expiration) are as expected.

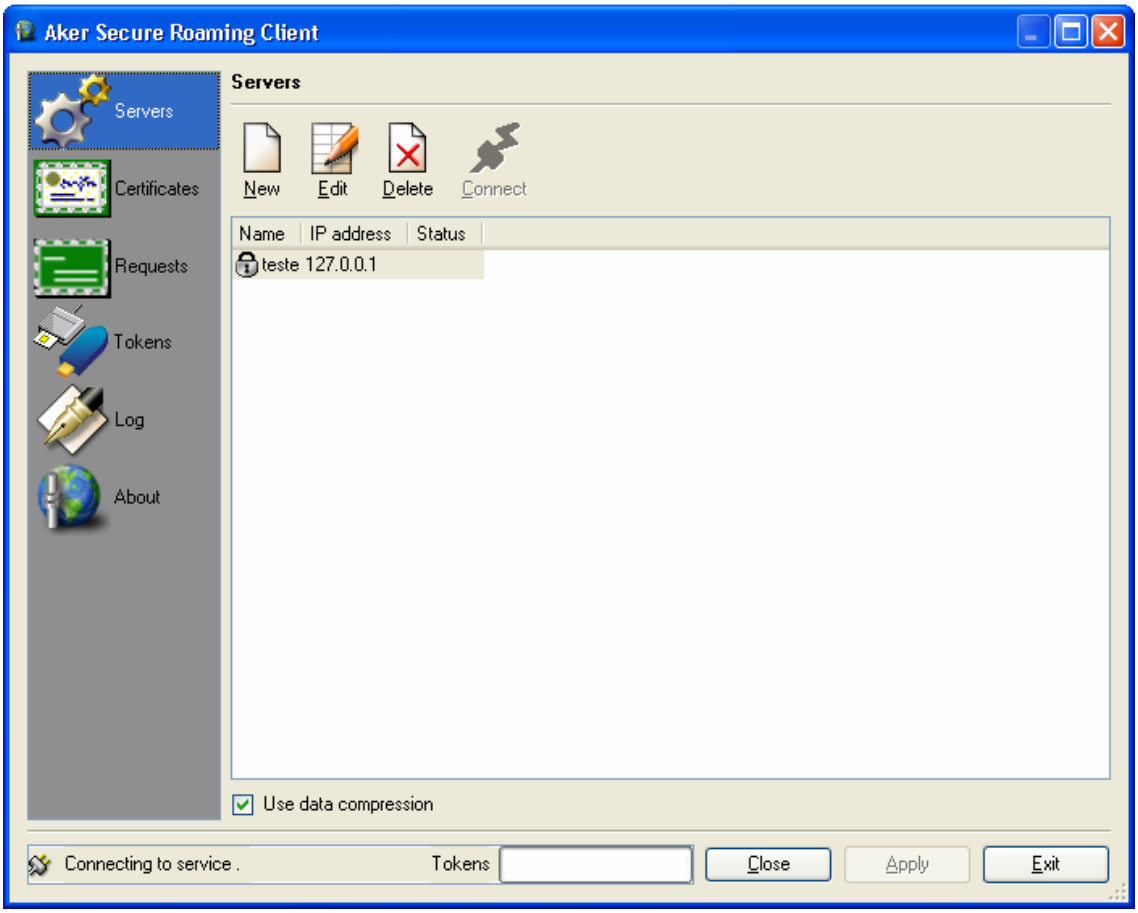
If you incorrectly type anything, your license will be considered invalid, you must type the license holder's name, IP address and key **exactly** as written in your license term.

Copyright (c) 2003-2005 Aker Security Solutions

3-0 Configuring and managing the Aker Secure Roaming Client

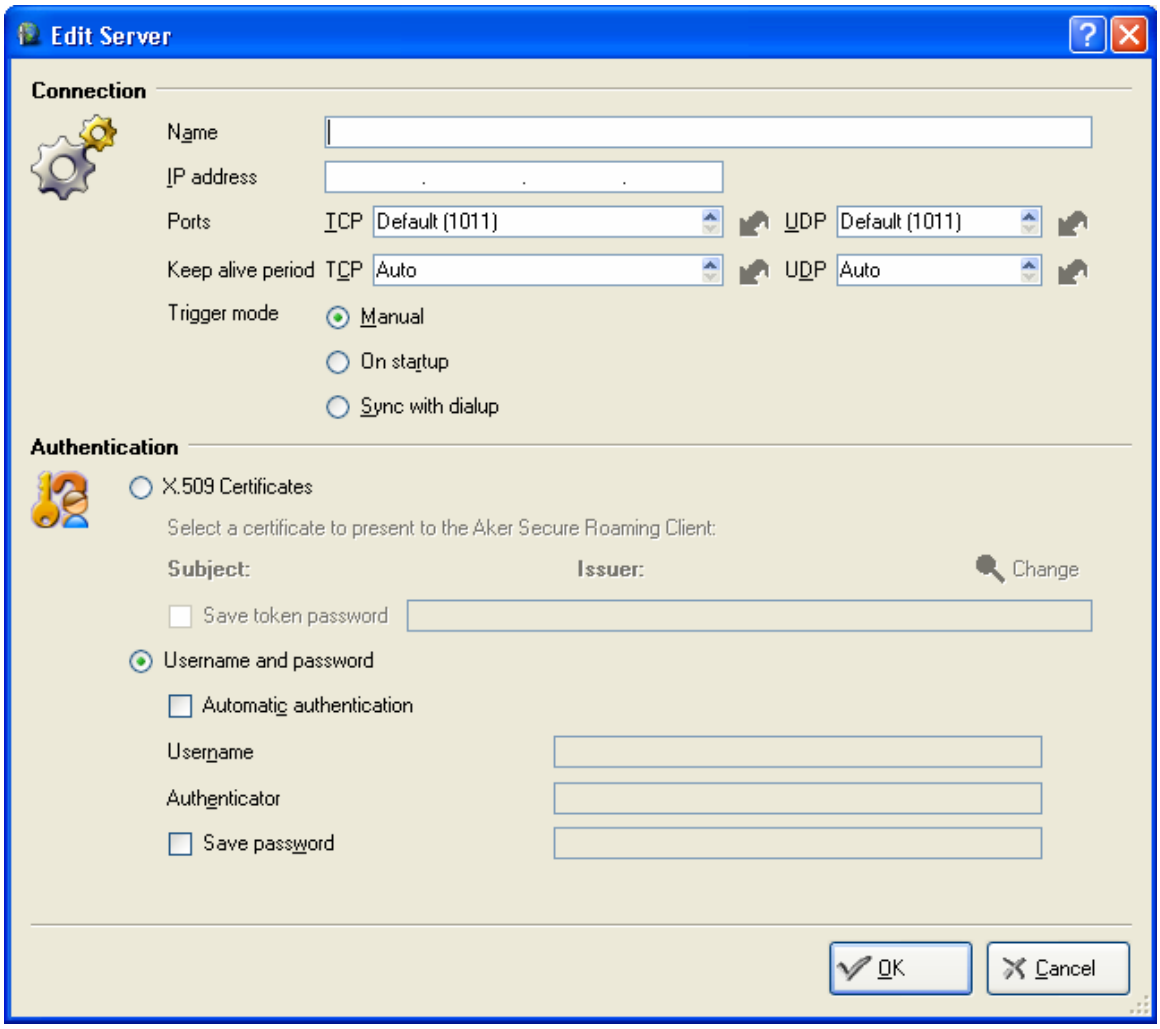
Here you'll find the necessary instructions to correctly configure and manage your Secure Roaming Clients. You shall discover they are much simpler than the Server, thereby making end-user's experience much simpler.

3-1 Servers page



In this page you'll find a place to inform the client on which servers it shall connect, and when to do so. Apart from the servers' list, there are buttons to add, edit, remove and connect/disconnect from the servers.

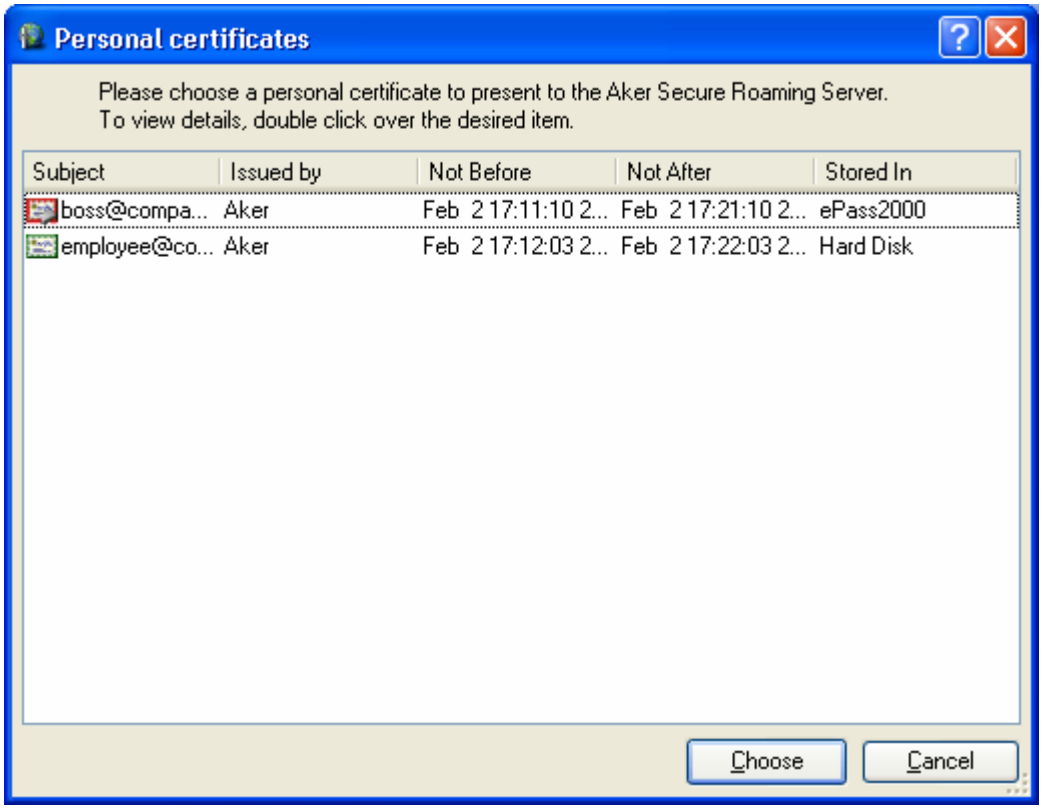
By clicking on **new** or **edit** you'll be prompted with the following dialog:



- **Name**: This name is for your reference only. It can be anything which helps identifying the Secure Roaming Server you are connecting to.
- **IP Address**: The server's IP address, as seen from the client. This number can be different from the server's real address, if it is placed behind a NAT gateway. Please note you won't be able to type anything else but an IP address in this field.
- **Ports**: The TCP and UDP ports the server is listening on. These numbers must match the ones entered when configuring the server, or, like the IP address, the translated port numbers if the server is behind a NAT engine which changes the ports.
- **Keep-alive period**: This period is the maximum period of inactivity in the TCP connection and UDP packet sequence. If the default values are too big, so that any equipment between the client and the server either drop the connection or change UDP port numbers (typical in a IP masquerading device -- N-1 NAT -- near to the client), please decrease them accordingly. Please keep in mind that using a very short number *just to be sure* is hardly a good idea, because you may end up using much of the scarce bandwidth between the client and the server with keep-alive packets.
- **Trigger mode**: This setting defines when the VPN connection should be started and ended. There are three choices:

1. **Manual**: The connection will be setup and tear-down whenever the user chooses to do so. If some problem makes the connection stop, the user will have to restart it manually.
2. **On startup**: The client will try to maintain the connection always active from the time it is started on. This method is more useful for clients connected to permanently to the network, like DSL lines or local area networks.
3. **Sync with dialup**: (*Windows OSes only*) The connection state will be synchronized with the dial-up adapter's. This is the preferred method for users which cannot get access to a permanent Internet connection. In this method, the system will always try to keep the VPN session alive if there is a dial-up connection active.

- **Authentication**: You can choose between two methods to authenticate yourself
  - **X.509 Certificates:** While operating in this method, you need a correctly installed X.509 certificate to present to the Secure Roaming Server. To select one of such certificates, click on the **Change** button. The following dialog will be shown:



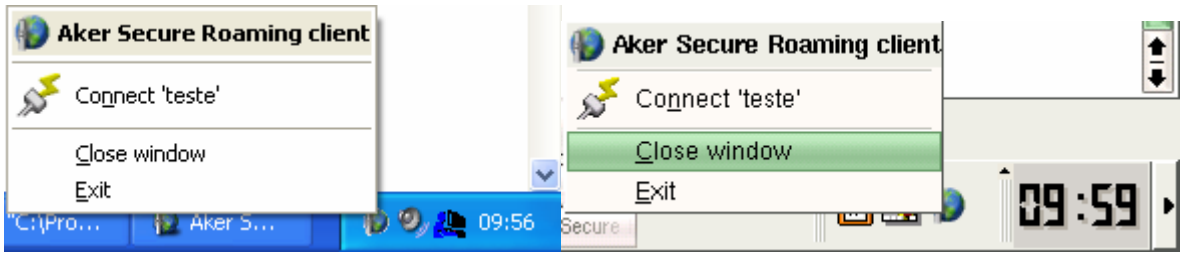
    The dialog will be filled with a list of possible certificates. To choose one of them, double-click on it or click the **Choose** button.

    - **Save token password:** This option will be enabled only when the selected certificate is stored in a external cryptographic token. It makes the Client store your token password in encrypted form, so that you do not have to type it upon VPN session establishment.
  - **Username and password:** This is the traditional authentication mechanism: the user presents the server a username / password pair,

which is verified. If you do not fill the fields bellow, you will be prompted for them upon connection establishment.

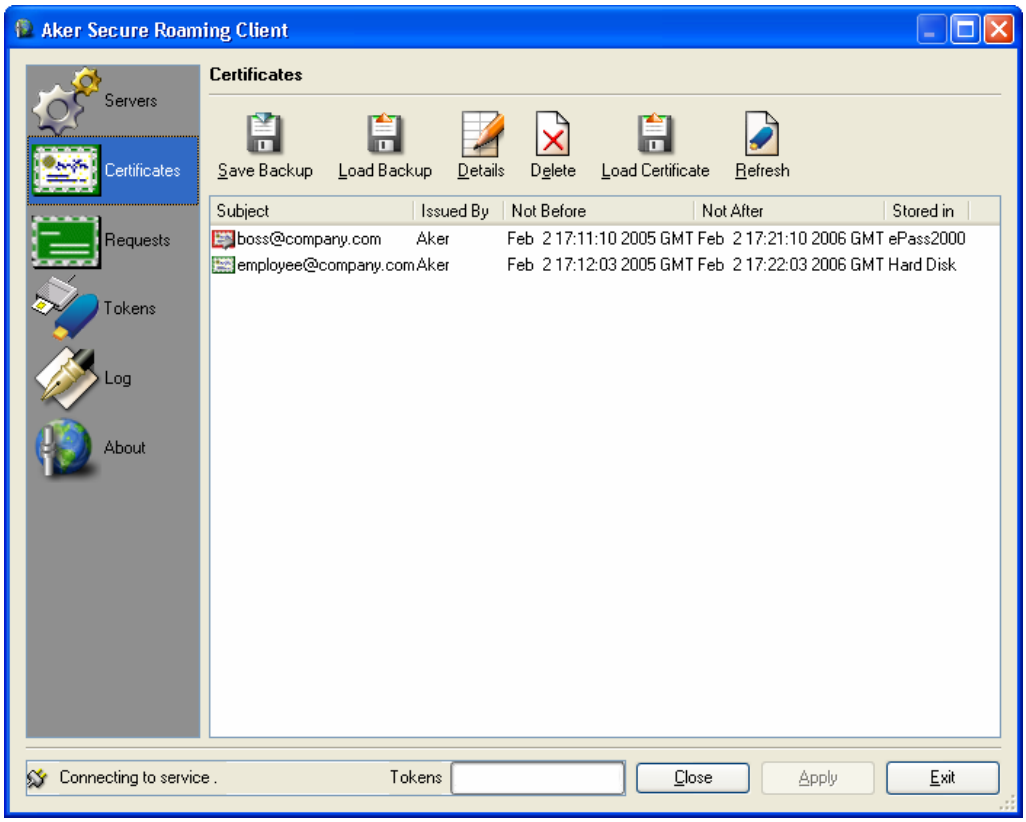
- **Username**: your username on the network you are connecting to.
- **Domain**: the authenticator name used in the server. If you leave this field blank, the server will try every authenticator it knows about.
- **Password**: your password can be save, so that you need not to enter any information when the VPN session is established. If you check this method, please be aware your password will be saved in encrypted form. Using this options will enable you to run the client without the graphical user interface (just the background daemon/service), which can be particularly useful for Unix users no willing to start an X session.

Some of this page's functionality can be accessed by right-clicking the system tray icon:



3-2 Certificates page

This page makes it possible for you to manage the certificates used for authentication. The page has the following appearance:



The available actions are: **Save Backup**, **Load Backup**, **Details**, **Remove**, **Load Certificate** and **Refresh**.

- The **Save/Load Backup** buttons save or restore a certificate and its private key using the PKCS#12 format. This format is an encrypted package for both the certificate and the corresponding keys. To save or restore it, a encryption/decryption password must be entered. If you forget the password used when saving the backup, you will not be able to load it.
- The **Details** button make a new dialog pop up with additional information about the certificate subject and issuer.
- The **Remove** button erases the certificate and its private key. If the certificate is stored in an external hardware token, you will be prompted for the token PIN or password.
- The **Load Certificate** button loads a certificate, which can be stored both in DER or Base64 formats. This certificate is generated by a CA, using a previously created request.
- The **Refresh** button is only useful if you are using a external hardware token. It will search all installed tokens for ready to use certificates. During this process, an animated bar will be shown on the bottom of the window. The bar will stop when the refresh operation is complete.

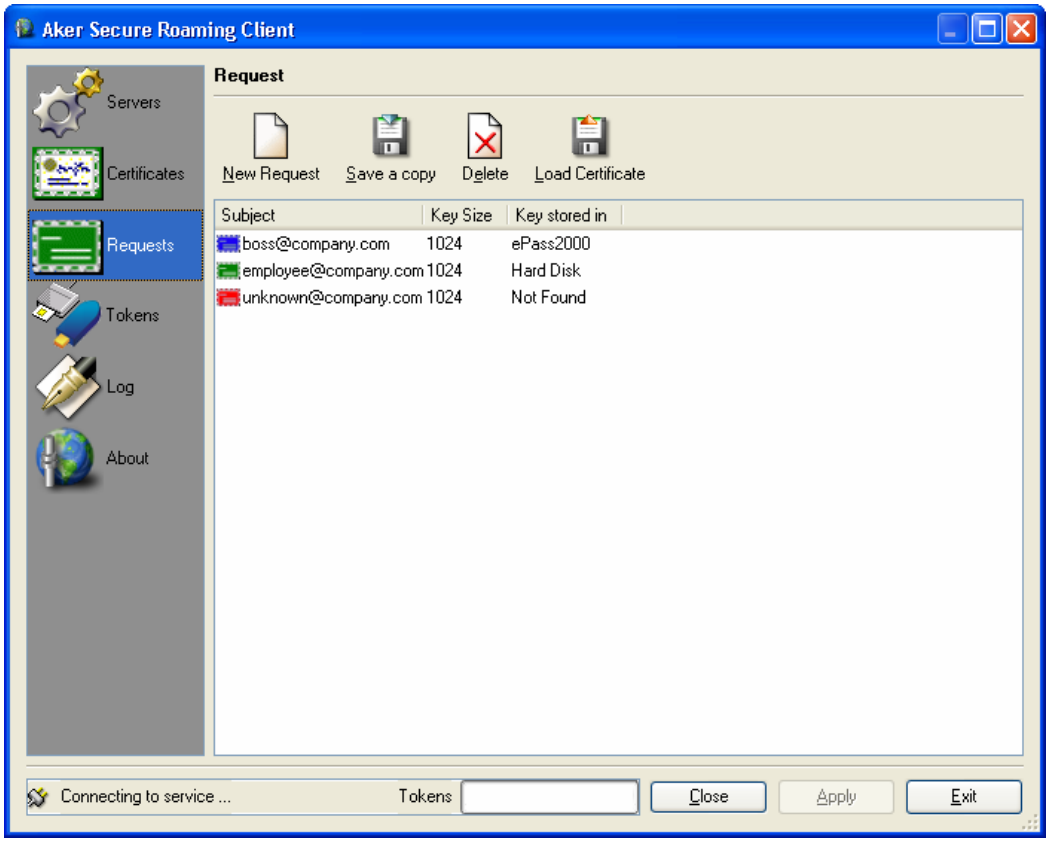
According to the certificate and private key location, a different icon is displayed left of the certificate subject name:

- Certificate and private key stored in hard drive. The files can be found in the x509 folder inside the installation path.

- Certificate and private key stored in an external hardware token. The token name will be shown on the *Stored in* column.

3-3 Requests page

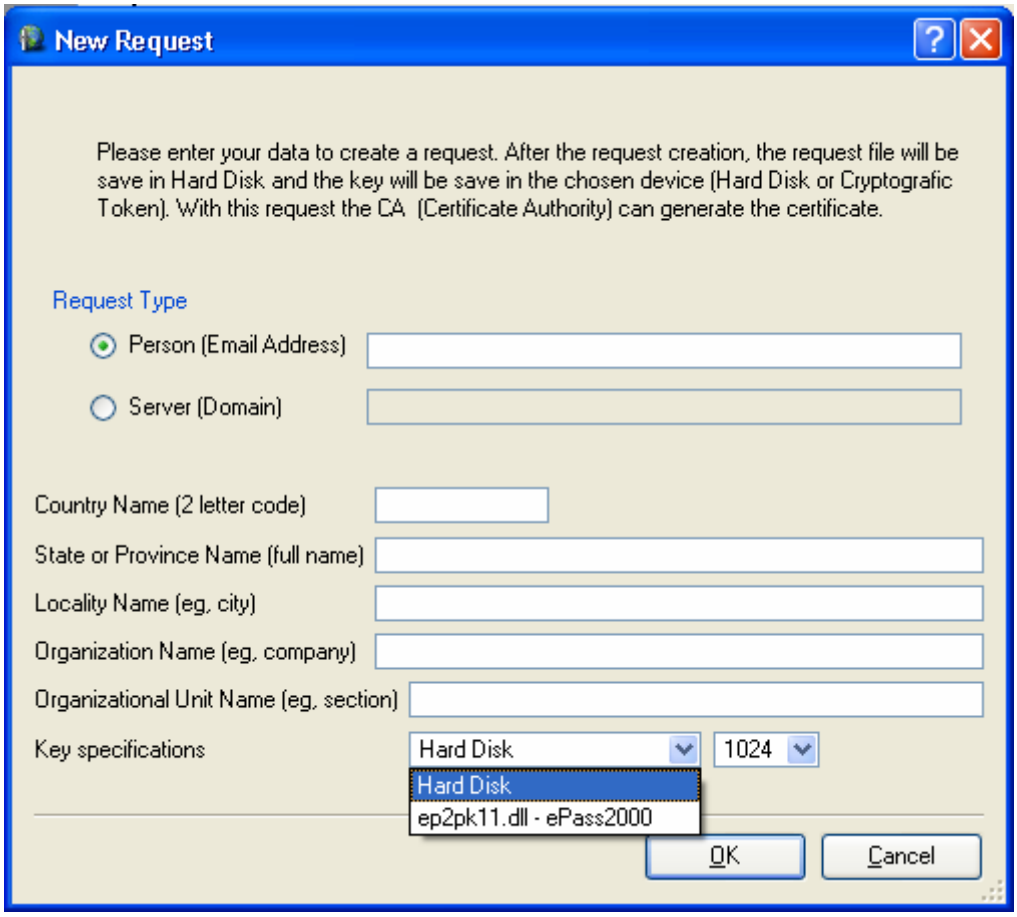
This page allows you to create and manage the certificate requests.



The avaiable options are: **New Request**, **Save a copy**, **Delete** and **Load Certificate**:

- **New Request**: Prompts the user for the data necessary to generate a new certificate request and the corresponding key pair.
- **Save a copy**: Exports the request using a standard format used by CAs. The file saved here can be taken to a CA in order to obtain a certificate.
- **Remove**: Deletes the saved request and key pair from wherever it is installed. If the store location is a external hardware token, the user will be prompted for the token password.
- **Load Certificate:** loads a certificate, which can be stored both in DER or Base64 formats. This certificate is generated by a CA, using a previously created request.

The dialog box used to prompt the user for certificate request information is the following:


New Request
Please enter your data to create a request. After the request creation, the request file will be save in Hard Disk and the key will be save in the chosen device (Hard Disk or Cryptografic Token). With this request the CA (Certificate Authority) can generate the certificate.
Request Type
Person (Email Address)
Server (Domain)
Country Name (2 letter code)
State or Province Name (full name)
Locality Name (eg, city)
Organization Name (eg, company)
Organizational Unit Name (eg, section)
Key specifications
Hard Disk
1024
Hard Disk
ep2pk11.dll - ePass2000
OK
Cancel

- **Request type:** Defines if the certificate requested is for someone or a server. The only difference is on the fields used for identification.
- **Country**: two letter country code (e.g. BR for Brazil).
- **State or Province:** the province or state full name.
- **Locality name:** the city or district full name.
- **Organization name:** Company full name (e.g. Aker Security Solutions)
- **Organizational Unit Name:** Department or section full name.
- **Key specifications:** The user can choose where to store the private key (hard disk or a external cryptographic token) and the key size in bits.

  The key generation process can be very time consuming, depending on key size and key storage media. During this operation, the window will be disabled (grayed out) until it is complete. Please wait for the window to close before using the client again.

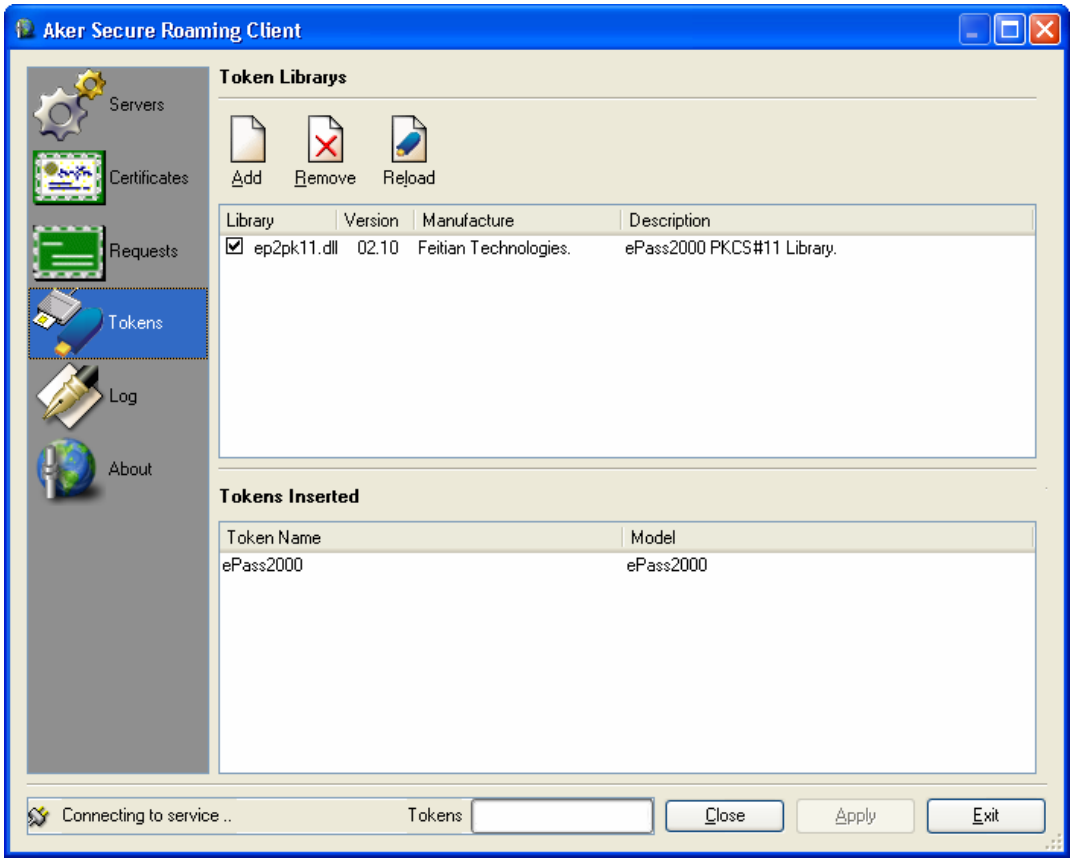
According to the key storage media, one of the following icons will be shown next to each request:

- Keys stored on the hard disk. The private key is saved inside the x509 folder on the installation path.
- Keys stored on external cryptographic tokens. The token where the key is stored will be shown on the *Key Stored in* column.
- Private key not found. The key can be lost, damaged or stored in a token which is not currently connected to the system.

A request with a not found key is not necessarily invalid. If it is stored in an external token which has been removed from the system, it will be available again (blue) when the token is inserted and the refresh button is pressed.

3-4 Tokens page

In this tab you can manage the PKCS#11 dynamic libraries used to access the hardware tokens. These libraries are like drivers and are provided by the token manufacturer. You can also view which tokens are inserted and recognized by the system.



In the top box the PKCS#11 libraries are displayed. In the bottom one, the currently detected tokens are displayed. The bottom box cannot be directly edited, it will change its contents automatically when the **Reload** button is pressed.

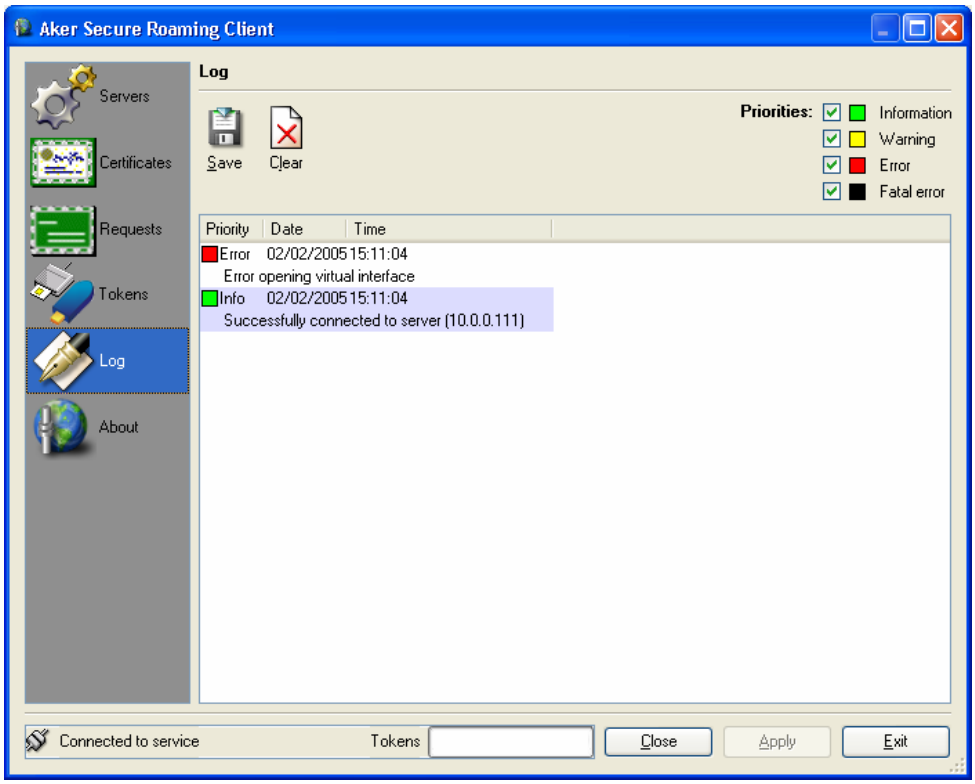
The available options for managing libraries are **Add** and **Remove**.

Only when the library is loaded and enabled (checked), the tokens which it is responsible for will be detected.

To load a new library, click on the Add button and browse for the .dll (windows) or .so (Unix) file. Next, click on the square box next to it, so that a checkmark is drawn inside it. Finally, click Reload, so that the tokens are recognized. To be sure you selected the correct file, please verify if the additional columns (version and description) are filled. If a dynamic library for another purpose is selected by mistake, a error message will be displayed.

If you have trouble finding the correct library file for your token, please contact the token manufacturer or reseller. They can provide you with support on finding theses files.

3-5 Log page



This page shows you the client's activity log. This can be very useful for the system administrator when troubleshooting a malfunctioning setup. Clicking the *Save* button will allow you to export the log to a text file which can easily be sent to your support personnel.
By toggling the colored marks on the top-right, you can control which new messages will be shown on the log window. Please note that messages already in the log list can only be removed by clicking the *Clear* button.

Copyright (c) 2003-2005 Aker Security Solutions